



Virtualisation de serveurs à l'aide d'un logiciel de cloud

M. Jouvin, G. Philippon

► To cite this version:

M. Jouvin, G. Philippon. Virtualisation de serveurs à l'aide d'un logiciel de cloud. JRES 2011 "Journées Réseaux", Nov 2011, Toulouse, France. in2p3-00702961

HAL Id: in2p3-00702961

<https://hal.in2p3.fr/in2p3-00702961>

Submitted on 31 May 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Virtualisation de serveurs à l'aide d'un logiciel de cloud

Guillaume PHILIPPON

Laboratoire de l'accélérateur Linéaire
Bât 200 – Université Paris 11
91898 ORSAY CEDEX

Michel JOUVIN

Laboratoire de l'accélérateur Linéaire
Bât 200 – Université Paris 11
91898 ORSAY CEDEX

Résumé

Depuis le début 2011, le LAL (Laboratoire de l'Accélérateur Linéaire) expérimente une gestion de type « cloud » (privé) de ses ressources informatiques, pour permettre la mise en œuvre de serveurs plus personnalisés tant pour les besoins des utilisateurs que pour les services centraux du laboratoire, avec une allocation dynamique des ressources physiques disponibles. Entre autres, nous avons utilisé la virtualisation de notre infrastructure web, actuellement cent sites web sur quelques machines physiques, comme projet de validation des potentialités de l'approche « cloud privé ». Cette gestion dynamique présente l'avantage de fournir potentiellement la haute disponibilité, sans avoir à recourir à des technologies de clustering complexes.

La mise en place de ce « cloud privé » au LAL s'appuie sur le projet européen FP7 StratusLab, qui sera décrit dans cet article. StratusLab développe une plateforme opensource permettant la mise en œuvre de « cloud » de type IaaS ("Infrastructure as a Service"). La plateforme StratusLab fournit des services innovants comme la certification d'image virtuelle de référence (Marketplace), une interface utilisateur simple pour l'utilisation du cloud et une API implémentant les principaux standards d'accès aux ressources d'un cloud (OCCI, CDML...). Elle fournit aussi l'intégration avec des outils de gestion de configuration, tels Quattor[2]. Afin de garantir un développement qui suive au plus près les besoins des utilisateurs et des administrateurs de site, le projet StratusLab utilise une méthodologie agile de développement logiciel, qui permet une réponse rapide aux différents besoins à travers des cycles de développement courts et des releases fréquentes.

1 Introduction

Les technologies de cloud connaissent un succès grandissant ces dernières années pour deux raisons complémentaires :

- Elles permettent d'accéder à la demande à de grandes quantités de ressources aisément configurables, sans avoir à se soucier de leur « provisioning ».
- Elles permettent aux centres de traitement de données d'optimiser leurs investissements en donnant accès à des ressources qui sinon resteraient inutilisées.

Cependant, l'utilisation d'un cloud public présente certains inconvénients. Par exemple, le dépôt de données dans un cloud public dont on ne maîtrise pas les ressources peut poser des problèmes de confidentialité.

Le projet StratusLab[1] a pour objectif de construire un logiciel open source qui permette de mettre en place un cloud privé de type Infrastructure as a Service (IaaS). Le projet offre un jeu de commandes simples pour l'interaction avec le cloud ainsi que des scripts de configuration ou, alternativement, une intégration dans l'outil de déploiement Quattor[2], qui assurent une mise en place rapide du cloud.

2 Les clouds

Le terme cloud est utilisé pour décrire plusieurs types d'infrastructure répartie :

- IaaS (Infrastructure as a Service) : ces infrastructures proposent des services de machines virtuelles, de stockage et de gestion de l'accès réseau. Ce type d'infrastructure permet une prise en main rapide d'une nouvelle machine. L'objectif étant de fournir un environnement virtuel proche de l'environnement réel, il n'est pas nécessaire de modifier les applications utilisateurs pour profiter de cette plateforme. Néanmoins, il laisse à la charge de l'utilisateur le soin de créer son image virtuelle ce qui peut être un frein.
- PaaS (Platform as a Service) : il s'agit de proposer des services (généralement implémentés comme des web services) qui permettront de construire des applications s'appuyant sur des services distribués. La gestion de la répartition des calculs ou du stockage est déléguée à la plateforme : l'application ne les gère pas directement et bénéficie de l'« élasticité » inhérente à la plateforme. Il s'agit de technologies comme Google Apps Engine.
- SaaS (Software as a Service) : ces infrastructures sont en relation directe avec l'utilisateur d'un logiciel. On a tendance à qualifier de SaaS toute application implémentée à travers un portail Web. Il s'agit d'applications comme Google Mail, Google Calendar ou Google Doc.

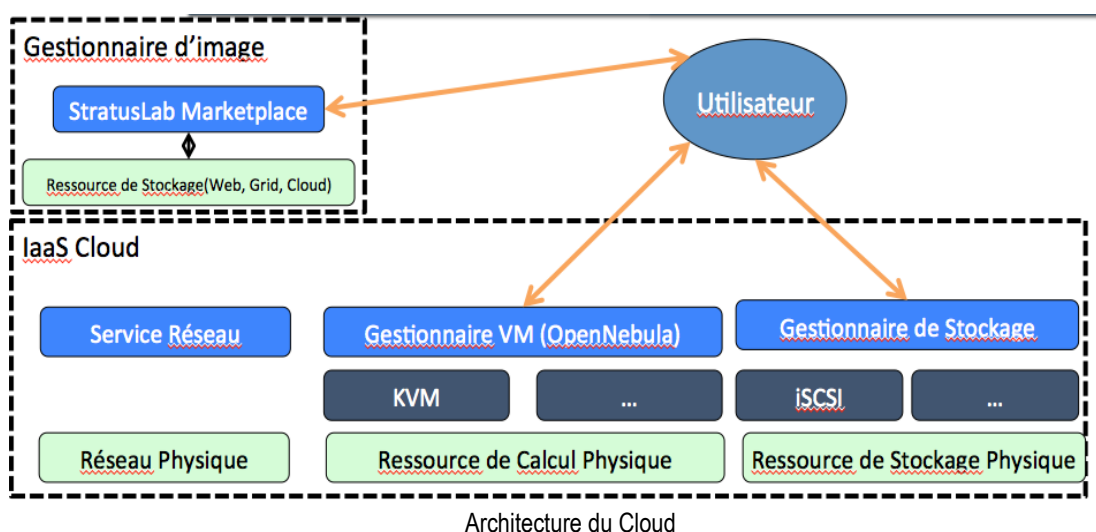
Ces trois types de cloud sont souvent vus comme trois niveaux fonctionnels différents : les services SaaS peuvent s'appuyer sur une plateforme PaaS ou IaaS et une plateforme PaaS s'appuie généralement sur une infrastructure IaaS.

L'investissement utilisateur est aussi très différent dans les trois types de cloud. Avec un cloud SaaS, l'utilisateur bénéficie d'une application « clé en main » ne nécessitant pas de compétences d'installation particulières de sa part. Dans un cloud PaaS, il va pouvoir se concentrer sur le développement des fonctionnalités spécifiques à ses besoins, en s'appuyant sur des services qu'il n'aura pas à maintenir (de ce point de vue, cela ressemble aux services offerts par un middleware de grille). Enfin, les plateformes IaaS permettent de profiter des avantages d'un cloud sans développement particulier (les machines virtuelles pouvant faire fonctionner n'importe quel programme), mais elles nécessitent plus d'investissement de la part des utilisateurs qui devront assumer la gestion de la configuration de ces machines.

Enfin, la notion d'élasticité est un des grands bénéfices apportés par le cloud. L'élasticité est la capacité qu'a un cloud à s'adapter aux besoins temporaires d'un utilisateur en matière de calcul ou de stockage. Afin de répondre à un pic de charge, un utilisateur peut facilement augmenter le nombre de nœuds de calcul, puis ensuite les relâcher dès que le besoin est résorbé.

3 L'infrastructure de StratusLab

Le projet StratusLab fournit les services de base d'un cloud IaaS. Ainsi, il propose une infrastructure de gestion de machines virtuelles, une infrastructure de gestion de stockage ainsi qu'une gestion des accès réseaux. En plus, StratusLab offre d'autres services avancés comme, par exemple, le Marketplace qui est un moyen de mettre à disposition des images virtuelles de référence certifiées (signées) associées à une description de leur contenu.



3.1 L'infrastructure de gestion de machines virtuelles.

L'infrastructure de gestion de machines virtuelles est le cœur d'un cloud IaaS. L'objectif de cette infrastructure est de permettre de faire fonctionner une machine virtuelle sur une machine physique. Elle se compose généralement de machines de contrôle appelées « master » et de plusieurs machines qui vont effectivement instancier (faire tourner) les machines virtuelles appelées « hyperviseurs ». Il est classique de considérer qu'à un cœur physique de l'hyperviseur correspond un CPU virtuel. Un hyperviseur comprenant 24 cœurs peut donc instancier typiquement 24 machines virtuelles.

StratusLab utilise OpenNebula[3] comme gestionnaire de machines virtuelles. OpenNebula fournit une API XML-RPC permettant le contrôle à distance. De plus, il contient un système de *contextualisation* qui permet de personnaliser une machine virtuelle. Ainsi, une même image virtuelle pourra être utilisée de plusieurs façons différentes selon la contextualisation qu'on lui appliquera.

Le cycle de vie des machines virtuelles est géré par OpenNebula. L'utilisateur pourra créer une machine virtuelle, vérifier son état ou bien encore la détruire. L'administrateur de site pourra lui faire migrer une machine virtuelle d'un hyperviseur à l'autre, l'arrêter momentanément ou bien la détruire.

Le projet StratusLab a ajouté un certains nombres de services à OpenNebula :

- une fonctionnalité de *quarantaine*, qui permet de conserver pendant une durée configurable les images des machines virtuelles ayant été détruites. Ceci permet, en cas de problème de sécurité, de pouvoir faire une analyse post-mortem de la machine virtuelle.
- Authentification par certificat en alternative au password

3.2 L'infrastructure de gestion de stockage

De façon générale, la gestion du stockage dans un cloud peut être vue selon deux approches :

- La mise à disposition de fichiers : Il s'agit de service comme NFS ou WebDav, les utilisateurs ont accès à un espace où ils voient un ensemble de fichiers
- La mise à disposition de disque « brut » : dans ce cas, la machine virtuelle monte un espace de type disque utilisable sans système de fichier préinstallé.

StratusLab propose l'approche de type disque. Cependant, le projet a différencié trois types de stockage :

- Les disques volatils
- Les disques statiques
- Les disques persistants

Les disques volatils sont des disques qui suivent le cycle de vie de la machine virtuelle. Ils sont créés à l'instanciation de la machine virtuelle et sont détruits à l'arrêt de celle-ci. Il s'agit, typiquement, de disques permettant le stockage de données temporaires.

Les disques statiques sont des disques qui peuvent être montés par une ou plusieurs machines virtuelles. Ils ne sont accessibles qu'en lecture. Ce type de disque est habituellement utilisé pour mettre à disposition des bases de données ou des jeux de données qui vont être utilisés par plusieurs machines virtuelles.

Enfin, les disques persistants sont des disques qui possèdent leur propre cycle de vie. Basés soit sur l'utilisation du protocole iSCSI, soit sur une infrastructure NFS qui met à disposition des images disques, ils permettent de rendre disponible à une machine virtuelle un espace de stockage persistant vu comme un disque local. Ce disque est « branché » sur une seule machine virtuelle à la fois. Le projet fournit un jeu de commandes ainsi qu'une API (REST c'est-à-dire basée sur http, ici https) pour la gestion des cycles de vie des disques persistants. Les disques persistants peuvent être montés au démarrage de la machine virtuelle ou en utilisant les fonctionnalités « hot-plug » du système après son démarrage.

Le service disque persistant est géré au niveau de l'hyperviseur. Celui-ci se charge de présenter le disque persistant comme un disque classique. Aucune configuration n'est requise sur la machine virtuelle, sauf pour le support de la fonctionnalité hot-plug sous Linux, qui nécessite l'installation du module acpiphp.

3.3 Le réseau

La virtualisation pose un problème particulier pour la gestion réseau : là où une machine 24 cœurs pouvaient faire tourner 24 programmes avec une seule adresse IP, un hyperviseur de même type dans un cloud va consommer 24+1 adresses IP si chaque application utilise sa propre machine virtuelle.

Afin de limiter l'impact sur le réseau de l'utilisation d'un cloud, StratusLab permet de distinguer trois types de connexion réseau pour une machine virtuelle :

- Les adresses IP publiques
- Les adresses IP locales
- Les adresses IP privées

Les adresses IP publiques sont visibles depuis l'extérieur du cloud. En conséquence, les machines qui les utilisent peuvent héberger des services accessibles depuis Internet, ce qui les rend vulnérables. Il est donc nécessaire que les images virtuelles de ces machines soient soigneusement sécurisées.

Les adresses IP locales ne sont visibles que depuis l'intérieur du cloud. Le réseau permet aux machines virtuelles de communiquer entre elles mais ne permet pas d'accès extérieur direct. Néanmoins, elles accèdent à Internet via une translation d'adresse (NAT). Elles peuvent, par exemple, permettre l'installation d'un cluster MPI sur le cloud.

Enfin, les adresses IP privées ne sont visibles que depuis l'hyperviseur faisant fonctionner la machine virtuelle. Comme pour les adresses IP locales, les machines correspondantes ont un accès à Internet via une translation d'adresse mais ne peuvent pas être vues d'Internet ou des autres machines virtuelles. Comme aucune interaction utilisateur ne pourra avoir lieu avec ces machines, la machine virtuelle doit être capable de récupérer ses données à traiter et déposer elle-même le résultat de son calcul dans l'espace de stockage. En contrepartie, les images virtuelles de ces machines nécessitent un niveau de sécurité moindre car elles ne sont pas exposées.

L'adresse IP est imposée par OpenNebula au démarrage de la machine virtuelle. Elle est assignée aléatoirement à partir d'un pool d'adresses IP défini dans la configuration OpenNebula. Il existe une option StratusLab pour définir une adresse IP statiquement au démarrage de la machine mais celle-ci n'est pas pour autant réservée. A l'avenir, un système de réservation d'adresse IP permettra à un utilisateur de s'assurer qu'une adresse IP ne sera pas utilisée par un autre utilisateur.

Plusieurs développements sont actuellement en cours dans le cadre de StratusLab pour améliorer la gestion du réseau. Tout d'abord, le « dynamic firewalling » permettra à un utilisateur de spécifier les règles de firewall qu'il veut voir appliquées à sa machine virtuelle. Actuellement, le gestionnaire de site définit une politique de firewall pour l'ensemble des machines virtuelles qu'il héberge. En permettant à l'utilisateur de spécifier ses propres règles, StratusLab vise à renforcer la sécurité des machines virtuelles.

3.4 Le Marketplace

Le service Marketplace a pour objectif de répondre à deux impératifs importants pour un cloud IaaS.

- Partager les images virtuelles
- Valider les images virtuelles

La création d'image virtuelle n'est pas simple. Elle doit répondre non seulement aux besoins d'un utilisateur qui n'est pas forcément expert en informatique, comme par exemple être compatible avec son application métier, et répondre aux contraintes de l'exploitation d'un parc informatique notamment en termes de sécurité. Pour beaucoup d'utilisateurs, la création d'image virtuelle est un frein à l'adoption d'un cloud IaaS.

Afin d'aider à l'utilisation des infrastructures de cloud, StratusLab propose un service de partage d'images de référence, le Marketplace. Ce service a pour objectif de fournir un ensemble de machines virtuelles avec une description de leur contenu (metadata), signées (numériquement) par leur créateurs et dont les administrateurs de site cloud peuvent accepter ou refuser l'instanciation.

Les machines virtuelles sont représentées par des métadonnées qui contiennent des informations sur l'image (hash md5 de l'image, signature du créateur, ...) ou son contenu (OS, logiciel installé, ...).

Ainsi, un utilisateur pourra faire « son marché » sur le Marketplace. Une interface web permet de rechercher une image virtuelle à l'aide de plusieurs critères. Le Marketplace dispose aussi d'une API REST, l'utilisateur pouvant ainsi développer des applications ou scripts pour interroger le Marketplace sans passer par une interface Web. Le langage de requête SPARQL[4] a été choisi par StratusLab pour formuler les requêtes lors de la recherche.

Les administrateurs de site ont la possibilité de limiter la variété des machines virtuelles qui peuvent tourner sur leur site. A l'aide des métadonnées disponibles sur le Marketplace, ils peuvent enforcer une politique d'utilisation de leur site. Ainsi, une image peut être refusée sur un site si l'administrateur considère cette image comme impropre à l'utilisation, et les images autorisées peuvent être restreintes à certains créateurs d'image.

Pour les créateurs d'images, le Marketplace est une opportunité de valoriser leur savoir faire. En plus de créer une image, ils doivent définir les métadonnées qui y sont attachées et signer ces métadonnées. De ce fait, ils mettent à disposition les images virtuelles qu'ils ont réalisées, le Marketplace devient la vitrine de leur travail. Les créateurs d'image sont responsables des images virtuelles qu'ils mettent à disposition et peuvent à tout moment les révoquer afin de les marquer comme obsolètes.

4 Utilisation de StratusLab au LAL

Le LAL, étant très impliqué dans le projet StratusLab, a choisi d'expérimenter depuis le début de l'année l'utilisation d'un cloud StratusLab pour la virtualisation de ses services internes. Pendant cette première phase visant à évaluer StratusLab comme plateforme de production, il a été décidé de se concentrer sur la virtualisation de quelques services :

- Service Web : le LAL héberge actuellement une centaine de sites Web sur deux machines physiques redondantes. Ces sites vont être progressivement transférés sur des machines virtuelles plus spécialisées. En effet, l'hébergement d'un grand nombre de sites aux pré-requis différents sur une même machine est une source de difficultés pour l'exploitation et la maintenance de ces serveurs du fait de la cohabitation parfois difficile entre certains modules
- Quelques services centraux cruciaux pour laquelle la haute disponibilité est requise : cette haute disponibilité sera implémentée à travers la migration automatique de machine virtuelle en cas de problème. Ces services sont notamment le serveur DNS, le serveur NIS et le service d'annuaire (LDAP).

Un objectif majeur du projet est de valider la capacité à implémenter des services hautement disponibles à travers la surveillance et la migration de machines virtuelles.

En fonction de l'expérience acquise durant cette première phase, nous envisageons à partir de 2012 d'augmenter les ressources physiques dans le cloud privé du LAL et d'implémenter de nouveaux types de services, en particulier les serveurs utilisés par les différents groupes de physique pour l'analyse de données. Chaque groupe utilise actuellement un pool de machines réservées exclusivement à son usage. Dans un souci de diminuer la consommation énergétique de notre salle machine, la virtualisation de l'ensemble de ces serveurs apparaît comme la voie privilégiée pour fournir un service « élastique » s'ajustant au mieux aux besoins réels d'un groupe pour une période donnée tout en optimisant le nombre total de machines.

En parallèle à ce cloud interne, il est prévu de déployer un deuxième cloud, lui aussi basé sur StratusLab, pour permettre la virtualisation des serveurs de calcul utilisés dans la ressource grille EGI installée au LAL (200 machines). Le but poursuivi dans ce deuxième cloud sera assez différent puisqu'il s'agira personnaliser l'environnement système de chaque application plutôt que d'imposer l'environnement fourni par le middleware installé (gLite) comme c'est le cas actuellement.

4.1 L'infrastructure de machines virtuelles

L'infrastructure de machines virtuelles du LAL se compose de deux hyperviseurs possédant 24 cœurs et 32 Go de RAM. Ceci permet d'instancier jusqu'à 48 machines virtuelles. Il est d'ailleurs prévu d'ajouter un troisième hyperviseur de même type dans le futur. Ce cloud est parfaitement extensible. Le LAL possède un cloud équivalent pour l'hébergement de l'infrastructure du projet StratusLab se composant de 10 hyperviseurs.

4.1.1 Les contraintes matérielles

Les principales contraintes matérielles de l'infrastructure de machines virtuelles sont liées au nombre et à la taille des images virtuelles que l'on souhaite instancier. En effet, l'infrastructure utilise actuellement un espace partagé pour le stockage des machines virtuelles en cours d'exécution. Si l'on souhaite instancier 48 machines virtuelles d'une taille disque de 10 Go, il faut :

- un espace commun de 480 Go,
- une haute disponibilité de cet espace pour que les machines puissent fonctionner,
- des performances d'accès soient suffisantes pour soutenir les charges IO.

Afin de répondre à ces critères, le LAL fait reposer cette partie de son infrastructure sur un SAN en RAID-6 connecté à 10 Gb/s.

4.1.2 Les contraintes logicielles

La gestion par le cloud des machines virtuelles constitue la principale contrainte logicielle. En effet, dans un système de virtualisation « classique », l'opérateur de la machine virtuelle peut suspendre l'exécution de sa machine et restaurer celle-ci dans l'état qui était le sien lors de sa suspension. Ceci est principalement dû au fait que l'opérateur de la machine virtuelle est aussi l'opérateur de l'hyperviseur.

Dans un cloud StratusLab, l'utilisateur de la machine virtuelle n'a qu'un contrôle limité de l'hyperviseur : il peut instancier (démarrer), vérifier le statut ou bien arrêter définitivement une machine virtuelle. Une fois arrêtée, la machine virtuelle ne disparaît pas entièrement mais est placée en quarantaine et seul l'administrateur du site peut avoir accès à cette image.

Ce mode de fonctionnement nécessite donc de préparer une image virtuelle complète et autonome, c'est-à-dire qu'il n'y ait pas besoin de l'intervention d'un opérateur pour relancer le service après redémarrage de la machine virtuelle.

Bien que contraignant, ce système se révèle en pratique un atout. En effet, en cas de compromission, de modification de configuration ou de toute autre action nécessitant une étude de l'image disque, l'opérateur de la machine virtuelle et l'administrateur du site peuvent se coordonner pour arrêter la machine virtuelle, redémarrer une image « saine » pour reprendre le service et étudier tranquillement l'image disque problématique.

4.1.3 La gestion de la haute disponibilité

Les systèmes de clustering actuels sont souvent complexes et nécessitent du matériel de haute qualité assurer une continuité de service. La virtualisation et par extension le cloud proposent une alternative simple à ces systèmes. En effet, la gestion des services par la virtualisation permet de déléguer au gestionnaire de machine virtuelle le contrôle de service en re-instanciant automatiquement un service en défaut plutôt que d'intégrer cette tâche à des services ce qui rend complexe leur configuration.

OpenNebula propose un module de supervision des machines virtuelles qui n'est pas exempt de bug. Le LAL a donc ajouté un monitoring permanent des VM qui se charge vérifier la disponibilité des machines virtuelles et d'instancier (redémarrer) les machines virtuelles en erreur.

4.1.4 L'élasticité des services

Afin de profiter de cette fonctionnalité, il est nécessaire de prévoir, dès la phase de conceptualisation d'un service, l'ajout ou la suppression de ressources à chaud. Les images virtuelles doivent pouvoir s'intégrer à l'infrastructure de service. Pour cela, nous utilisons la contextualisation qui permet de personnaliser une image virtuelle au moment de son instanciation. Par exemple, nous voulons pouvoir instancier temporairement un serveur Web pour un virtualhost particulier pendant la durée d'une conférence.

Pour illustrer le caractère opérationnel de cette caractéristique d'élasticité, on peut évoquer le cas d'usage suivant : le LAL a mis à disposition de deux laboratoires voisins, l'IPN d'Orsay et le CSNSM, son infrastructure de cloud dans le cadre d'une formation sur

l'installation et la configuration d'un système d'acquisition de données Narval[6]. Lors de cette formation, vingt cinq participants ont pu instancier chacun leur propre machine virtuelle « vierge » pour y installer et configurer leur système d'acquisition.

Le succès de cette formation a démontré le bénéfice de l'élasticité et le projet StratusLab souhaite proposer ce type d'utilisation aux formations organisées par le LAL.

Simplicité d'utilisation

Le choix de l'utilisation du cloud s'est fait dans le but d'offrir un accès simple à l'instanciation des machines. StratusLab, avec son jeu de commandes réduit et facile d'utilisation répond à ces critères. L'instanciation d'une machine se fait grâce à la commande

```
$ stratus-run-instance http://url/image-disk.img.gz
:: Starting 1 machine ::

:: Machine 1 (vm ID: 17)
    public IP: 134.158.73.236
:: Done! ::
```

Le statut d'une machine virtuelle peut être vérifié avec la commande

```
$stratus-describe-instance
id state      cpu    memory  public ip
17 Running    1      128     134.158.73.236
```

Enfin l'arrêt d'une machine virtuelle se fait avec la commande

```
$stratus-kill-install id
```

4.1.5 Simplifier les procédures de maintenance matérielle

La virtualisation, donc le cloud, simplifie la maintenance matérielle en découplant la partie logicielle de la partie matérielle. La possibilité de faire de la migration à chaud dans un cloud permet d'assurer le retrait ou l'ajout d'une machine sans interruption de service.

OpenNebula se repose sur la librairie libvirt pour assurer la migration à chaud. Cette fonctionnalité n'est accessible que par l'administrateur de site en se connectant au master OpenNebula avec la commande

```
$ onevm livemigrate vmId hostId
```

4.2 L'infrastructure de stockage

L'infrastructure de stockage du LAL s'organise autour de serveurs NFS centraux hautement disponibles (Cluster Tru64 et Sun Solaris, NetApp). Toutes les machines de service du LAL sont clientes de ces serveurs centraux qui stockent la configuration des services et leurs données. Dans le cadre du cloud privé dédié aux services internes, nous avons choisi de considérer qu'une machine virtuelle était identique à un serveur physique pour ce qui concerne l'accès au service NFS puisque les images virtuelles qui pourront être instanciées sur ce cloud seront restreintes à celles maintenues par le service informatiques du LAL.

Cependant, quelques services appelés à être virtualisés ne peuvent pas être configurés pour utiliser les espaces NFS, comme le service mail par exemple ou un service de base de données. Pour ce type d'utilisation, le LAL met en place une infrastructure iSCSI hautement disponible (NetApp) qui sera la base du service de disque persistant pour le cloud privé.

4.3 La gestion du réseau

Les adresses IP sont délivrées aléatoirement. En attendant le système de réservation d'IP de StratusLab, le LAL a décidé d'utiliser deux jeux d'IP pour ces machines virtuelles :

- une *adresse de management* : délivrée par StratusLab, cette adresse n'est pas utilisée pour la connexion au service ni pour l'accès de la machine virtuelle aux autres services du LAL.

- les *adresses de service* : ces adresses IP sont spécifiques aux services hébergés sur la machine virtuelle. Ce sont les adresses utilisées pour se connecter au service et pour la connexion de la machine virtuelle aux autres services du LAL comme, par exemple, le service NFS. Ces adresses sont configurées à l'aide du mécanisme de contextualisation d'OpenNebula. Ainsi, il ne sera pas nécessaire de créer autant d'images virtuelles qu'il y a de services différents : par exemple il ne sera nécessaire de créer qu'une seule image « serveur web » pour en instancier plusieurs servant des virtual hosts différents (utilisant des adresses IP différentes).

4.4 La configuration des machines virtuelles

Le LAL est impliqué dans le projet Quattor[2]. L'ensemble des services Linux du laboratoire sont gérés par ce système de configuration automatique. Pour faciliter la gestion des images, le LAL utilise Quattor pour décrire la configuration de l'image virtuelle (en général identique ou très proche de celle du serveur physique) et créer l'image. Par contre, à la différence des machines physiques, il n'est pas prévu de reconfigurer une machine virtuelle avec Quattor. Bien que cela soit possible, nous avons pris la décision de ne pas modifier les machines virtuelles en cours d'exécution. Cela nous garantit la cohérence entre nos images virtuelles et nos machines virtuelles en cours d'exécution. La mise à jour d'une machine virtuelle se fera en général par la création d'une nouvelle image, toujours avec Quattor, et le redémarrage de la machine virtuelle avec cette nouvelle image.

Pour plus d'information sur le fonctionnement de Quattor, vous pouvez vous référer à l'article Quattor[2].

4.5 Le Marketplace

Bien que le cloud du LAL décrit ici n'ait pas vocation à être ouvert aux utilisateurs ou à des personnes extérieures, il est envisagé de déployer un Marketplace « LAL » qui servira de dépôt des images et permettra leur gestion en fournissant les informations nécessaires à la traçabilité (créateur, date, informations sur le contenu) et en permettant la révocation des images obsolètes. Un Marketplace n'étant pas lié à un cloud particulier, l'infrastructure mise en place pourra être utilisée ultérieurement pour offrir un dépôt à d'autres utilisateurs du LAL par exemple pour produire des images utilisables sur le cloud grille mentionné plus haut.

5 Conclusion

Le projet de virtualisation des serveurs est encore en phase de déploiement. Diminuer la complexité du processus de création des images est le principal défi qu'il nous reste à relever. Si configurer un service n'est pas plus difficile pour une machine virtuelle que pour une machine physique, le paramétrage de la contextualisation pour rendre le service « élastique » et donc tirer parti du cloud nécessite un effort particulier. L'utilisation d'un outil de gestion de configuration, comme Quattor, nous permet de construire une image virtuelle avec les mêmes procédures que celles qui étaient appliquées aux machines physiques.

StratusLab, en tant que projet européen a son propre calendrier, qui n'est pas forcément celui de notre projet. Cependant, globalement, les solutions fournies par StratusLab répondent aux attentes du LAL, et, les procédures mises en place dans le cadre du projet de virtualisation des serveurs dépendent peu des spécificités de StratusLab. Elles pourraient être facilement adaptées à d'autres solutions de cloud privé comme OpenStack[5].

Les solutions apportées par StratusLab permettent d'assurer une meilleure utilisation des ressources informatiques tout en garantissant la sécurité des services. En particulier, le Marketplace est l'élément central de la stratégie de sécurité de StratusLab. En fournissant des images standardisées des services, il assure la cohérence des configurations, une gestion des mises à jour simplifiée ainsi que l'intégrité des systèmes.

Enfin l'approche cloud privé nous a permis d'évoluer dans notre réflexion. Au début, nous pensions réserver l'usage du cloud au service informatique seul, nous envisageons désormais de l'ouvrir aux utilisateurs du LAL.

6 Bibliographie

Charles Loomis, Mohamed Airaj, Marc-Elia Bégin, Evangelos Floros, Stuart Kenny, David O'Callaghan. *StratusLab Cloud Distribution*. To appear as a chapter of *European Research Activities in Cloud Computing* : March 2012

[1] <http://stratuslab.eu/>

- [2] Michel Jouvin, *Quattor* : JRES 2011 – <http://www.quattor.org>
- [3] <http://opennebula.org/>
- [4] <http://www.w3.org/TR/rdf-sparql-query/>
- [5] <http://www.openstack.org/>
- [6] <http://narval.in2p3.fr>